FILED

OCT 06 2017

PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY ______ DEP CLK

UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Alcatel One Touch, Model 2017B cellular flip- phone

Case No. 5:17-MJ-1900-RN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A

located in the Eastern District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:
See Attchment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession with the Intent to Distribute Heron

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: __________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Tanisha M. Jeter
Printed name and title

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means and was placed under oath.

Date: October 6, 2017
City & State: Raleigh, North Carolina

Robert T. Numbers, II United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF a **Alcatel One Touch Model 2017B cellular flip-phone**	Case No. 5:17-MJ-1900-RN

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Tanisha M Jeter, Special Agent with the Bureau of Alcohol, Tobacco, and Firearms ("ATF"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I, Tanisha Jeter, am employed as a Special Agent for the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been since 2015. I have been a sworn law enforcement officer since 2012 working in a criminal investigator capacity the length of my career. During my employment with ATF, I have conducted several investigations related to federal firearms and narcotics violations. Through training and experience while working these cases, I have learned that computers, cellular phones, tablets and other electronic storage devices often contain evidence of crimes. Cellular phone histories often contain evidence related to requests for sale and delivery of narcotics, internet activity, financial transactions, package tracking information, and addresses of where narcotics or money originates or has been shipped. Additionally, cellular telephone SMS (Text) histories often contain conversations between the source of supply and customers related to firearms trafficking or narcotics trafficking. Suspects

of criminal activity often communicate with accomplices and/or victims before and after their crimes via cellular devices. Further, photos and videos stored therein depicting firearms, large amounts of currency, and/or controlled substances are also shared via text messages and social media sites between sources of supply and customers.

2. I make this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — that is, electronic devices and media — which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachments A and B.

3. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant, and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched includes:

   a. Alcatel One Touch Model 2017B cellular flip-phone, hereinafter referred to as the "Device". The Device is currently located in the ATF Raleigh Field Office evidence vault.

5. The applied for Warrant would authorize the forensic examination of the Device as described in Attachment A, for the purpose of identifying electronically stored data as more particularly described in Attachment B.

PROBABLE CAUSE

6. As part of an on-going investigation into drug sales (heroin) by Qua'moria DAVIS, Henderson Police Department detectives utilized a confidential informant to contact DAVIS on DAVIS' cellular phone in February 2017 to order and purchase heroin from DAVIS.

7. In July 2017, Henderson Police Department detectives again utilized a confidential informant to contact DAVIS on DAVIS' cellular phone to order and purchase heroin from DAVIS.

8. On May 27, 2017, Special Agents (S/A) of North Carolina Alcohol Law Enforcement assisted North Carolina Highway Patrol in conducting license checks in Vance County North Carolina, along Highway 39 near Phyliss Lane. At approximately 12:35am, a dark blue Dodge Charger with Florida registration plate HBL-509 approached the checkpoint which was well lit by multiple law enforcement vehicles parked alongside the highway with blue lights activated. The vehicle was occupied by two (2) males; driver, Kermaine Hargrove Jr., (hereinafter "Hargrove") who produced a license for North Carolina Alcohol Law Enforcement S/A Wiggs, and front passenger, Qua'moria DAVIS, (hereinafter "DAVIS").

9. While S/A Wiggs spoke to Hargrove, S/A Wiggs could smell a very strong odor of marijuana emitting from the vehicle. S/A Wiggs asked Hargrove if marijuana was in the vehicle. Hargrove answered, saying "No" and that he did not smoke. S/A Wiggs told Hargrove that he could smell the marijuana and that he needed to tell the truth. The passenger, DAVIS, interrupted and said that they had just smoked a blunt.

10. Hargrove complied with instructions from S/A Wiggs to park the vehicle. Both Hargrove and DAVIS were frisked for weapons. While the frisk was being conducted on DAVIS, a strong odor of marijuana emanated from his person. A bulge was located in his rear left pocket. When removed, the bulge was a plastic baggie containing marijuana. In DAVIS' right front pocket, $3,345.00 of US Currency was located. Upon further search, a lump was felt in DAVIS' front, right, watch pocket. S/A Wiggs asked DAVIS what the lump was. DAVIS did not answer. S/A Wiggs removed the lump and discovered five (5) wax paper envelopes, commonly known in drug trafficking as "bindles", containing an off-white powder believed to be heroin. The wax bindles were stamped with "Donald Trump" in red letters. DAVIS looked at the wax bindles and said that he "forgot those were in there".

11. The subsequent search of the vehicle yielded a marijuana blunt in the passenger side door, along with three (3) cellular phones belonging to DAVIS. The marijuana, bindles containing what appeared to be heroin, US currency, and three (3) cellular phones were collected as evidence.

12. DAVIS has been arrested multiple times throughout 2016 and 2017 on drug trafficking, drug possession, and firearms violations. These violations include possession of stolen firearms, possession with the intent to distribute numerous bindles of heroin, and selling heroin to confidential informants.

13. Based on this investigation and based on my previous knowledge and experience, I know that suspects who possess narcotics and firearms illegally, will often utilize their cellular telephones to take photos of the illicit activity. Persons involved in the sale of narcotics also use

texts and other messaging services in the furtherance of their illicit activity. A forensic analysis of the above-listed device will therefore likely contain evidence of the alleged crimes.

14. The Device is currently in the lawful possession of ATF. The Device came into ATF's possession in the following way:

a. Device was seized by North Carolina Alcohol Law Enforcement following DAVIS' May 27, 2017 arrest following a traffic stop in which DAVIS was discovered in possession of what appeared to be heroin, a large amount of US currency, and marijuana. DAVIS confirmed that the Device seized belonged to him.

b. Henderson Police Department Detective, who is assisting ATF in the federal investigation of DAVIS, retrieved the Device from North Carolina Alcohol Law Enforcement on 9/6/2017 and stored the Device in the Henderson Police Department's evidence room.

c. ATF S/A Jeter retrieved the Device from Henderson Police Department's evidence room on 9/8/2017 and placed it in ATF Raleigh Field Office's evidence vault where it has remained.

15. Based on my training and experience, I know that the listed device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of North Carolina Alcohol Law Enforcement from DAVIS.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I know that the listed device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and/or PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. There is probable cause to believe that things that were once stored on the aforementioned Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit that there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this Affidavit supports probable cause for a search warrant authorizing the examination of the device as described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Special Agent Tanisha M. Jeter
Bureau of Alcohol, Tobacco, Firearms, and Explosives

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this written affidavit.
Dated: October 6, 2017

Robert T. Numbers, II
United States Magistrate Judge

ATTACHMENT A

This warrant authorizes the forensic examination and evaluation of the listed Device, an Alcatel One Touch Model 2017B cellular flip-phone, for the purpose of locating, identifying and recovering electronically stored information, as described more fully in Attachment B, incorporated herein.

The property to be searched is a cellular telephone described as follows: Alcatel One Touch flip-phone, Model 2017B, MEID DEC: 270 113 185 015 362 913; this phone is currently in the custody of ATF Raleigh Field Office, Raleigh, NC.

ATTACHMENT B

This warrant authorizes (i) the search of the property identified in Attachment A for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

(a) Evidence of violations of Title 21, United States Code, Section 841(a)(1) which was committed on or about May 27, 2017 by Qua'moria DAVIS; or

(b) Any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession in illegal due to the subject violations; or

(c) Any property designed for use, intended for use or used in committing any subject violations

Subject to the foregoing, the items authorized to be seized include the following:

1. Contents of the telephone directory;
2. Information and communications in the form of text, photographs, and/or images;
3. Phone call logs;
4. Stored communications and information to include voicemail, or any other memory feature;
5. Lists of customers and related identifying information;
6. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
7. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
8. All bank records, checks, credit card bills, account information, and other financial records;
9. Evidence of user attribution showing who used or owned the Device at the time the things described in this Warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
10. Records of Internet Protocol addresses used; and
11. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records or user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.